PAT-NO: JP411317734A

DOCUMENT-IDENTIFIER: JP 411317734 A

TITLE: DATA CIPHERING AND DECIPHERING METHOD AND NETWORK SYSTEM USING THE METHOD

PUBN-DATE: November 16, 1999

INVENTOR-INFORMATION:

NAME	COUNTRY
MIYAZAKI, SEIJI	N/A
TAKARAGI, KAZUO	N/A

ASSIGNEE-INFORMATION:

NAME	COUNTRY
HITACHI LTD	N/A

APPL-NO: JP11033760

APPL-DATE: February 12, 1999

PRIORITY-DATA: 10031636 (February 13, 1998)

INT-CL (IPC): H04L009/08, G09C001/00 , G09C001/00

ABSTRACT:

PROBLEM TO BE SOLVED: To obtain a secure and highly reliable secret distributing method by generating the common key of a common key cipher, ciphering information through the use of the ciphering and deciphering key, restoring the ciphering and deciphering key by a secret key belonging to each distributed secret holding person at the time of restoring the information, and restoring information through the use of the restored key.

SOLUTION: A computer 103 generates the random number (k) of a bit length
equal to the secret key and obtains an arithmetic result (x1, y1) by arithmetic
operation on an elliptic curve by an open key Q1 to the secret key d1 107 and
the random number (k). A hash function (h) is applied to the arithmetic result
(x1) to obtain a hash value h(x1), the data is ciphered with the value h(x1) as
the deciphering and ciphering key and the ciphered data C is stored in the file
111 of a file server 102. At the time of deciphering, the (x1, y1) are
obtained by arithmetic operation on the elliptic curve through the use of the
key of d1 107 and the function (h) is applied to x1 to restore a ciphering and
deciphering key h(x1) and ciphered data C is deciphered by using the key h(x1)
to obtain data M.